Department of Homeland Security Daily Open Source Infrastructure Report for 01 February 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports an explosion at a Florida defense contractor plant that makes ignition systems for aircraft engines exposed at least 100 people to krypton gas and sent 12 to the hospital for treatment. (See item 10)
- The New York Times reports a female ex−postal worker opened fire at a U.S. Postal Service mail processing plant in Goleta, CA, killing six people before committing suicide. (See item 18)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 31, Charlotte Observer (NC)* — **Utility seeks federal aid after Katrina.** Faced with staggering damages from the worst natural disaster in U.S. history, Entergy Corp. is attempting to recover from the loss of much of its New Orleans power market. The question of federal aid for the utility holding company is up in the air. Its Entergy New Orleans unit has sought bankruptcy protection. To increase customer bills −− one way to pay for $1.5 billion in damage to its transmission systems from hurricanes Katrina and Rita −− it must go through utility regulators. Entergy is hoping for federal help, similar to the $250 million ConEdison Co. received following the 2001 terrorist attacks in New York. It hasn't placed a dollar amount on

how much help it would like, but the company has warned that without assistance, New Orleans' customers could face rate increases of up to 140 percent −− a charge that economic developers say would stymie, if not kill, the city's recovery. The hurricanes downed power lines, flattened utility poles, and knocked out transmission systems throughout Entergy's Louisiana and Mississippi service territories, with approximately $80 million in damage. Only a fraction of Entergy's pre−Katrina power−customer base of 190,000 in New Orleans is expected to return in the foreseeable future.
Source: http://www.charlotte.com/mld/charlotte/business/13752375.htm

2. *January 31, Guardian (UK)* — **Experts raise safety fears over new generation of liquid gas terminals.** The UK government is continuing with plans to build a new generation of potentially dangerous gas importation terminals without exhaustive safety checks, industry experts warn. The issue has heated up since admissions by the UK gas company British Gas that cracks have been found on one of its new liquefied natural gas (LNG) vessels which forced it to return to the yard where it was built. Malcolm Wicks, the energy minister, said that safety was paramount, but critics believe they are being fast−tracked to prevent an energy shortage in Britain, which has seen soaring gas prices this winter and predictions of more trouble in 12 months' time. Chief concerns currently center on the construction of two LNG plants which within a few years could provide up to a quarter of Britain's gas supply. Critics claim that no full, open safety assessments have yet been done on how safe it is to have ships containing LNG in a harbor in Wales, though the terminals are planned to be operational by the end of next year. Opponents have argued that in an accident 20,000 people living in surrounding towns could be killed by burning gas.
Source: http://politics.guardian.co.uk/homeaffairs/story/0,,1698616, 00.html

3. *January 30, Reuters* — **Tribal militants blow up gas pipeline in Pakistan; third time this month.** Suspected tribal rebels blew up a gas pipeline in Pakistan's troubled southwest region on Sunday, January 29, shutting supplies to a U.S.− and British−owned power plant for the third time this month. The blast damaged a 24−inch diameter pipeline in the Naseerabad district in the southwestern province of Baluchistan, cutting off the gas supply to the nearby Uch private power plant. The main shareholders of the Uch plant are Britain's International Power Plc, and U.S. firms Tenaska Inc and GE Capital. It sells electricity to Pakistan's state−run Water and Power Development Authority. Tribal militants have frequently targeted gas facilities in the province, which is home to the Sui fields, Pakistan's main natural gas source.
Source: http://in.today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006−01−30T080045Z_01_NOOTR_RTRJONC_0_India−234421−1.xml&archived=False

4. *January 30, South Florida Business Journal* — **Florida Public Service Commission considers once−a−decade inspections for utility poles.** The Florida Public Service Commission (PSC) could order inspections every 10 years for all wooden poles that carry electric lines. The vulnerability of wooden utility poles to damage or failure during the 2004 and 2005 hurricane seasons could possibly be one of the major causes of extensive and protracted power outages, Commission chairperson Lisa Polak Edgar said. She added, "We have a responsibility to look for short−term and long−term answers that will reduce the impacts of storms on Florida's ratepayers." The commission could make a decision on inspection cycles in February. In a recommendation from commission staff filed Friday, January 27, the state's

investor−owned electric utilities and local telephone companies should inspect 10 percent of their wooden utility poles each year using specified techniques. The companies would have to report their findings to the commission. The recommendation notes federal guidelines for rural electric cooperatives suggest 10−year inspection cycles for wooden poles in most states and eight−year cycles in Florida.
Source: http://www.bizjournals.com/southflorida/stories/2006/01/30/d aily4.html

5. *January 30, Associated Press* — **Permanent members of UN Security Council agree on Iran nuclear review.** The United States and other permanent members of the United Nations Security Council agreed Tuesday, January 31, that the International Atomic Energy Agency (IAEA) should review Iran's disputed nuclear program and impose sanctions, if necessary. The Security Council meets Thursday, February 2 to debate the issue and to vote. The IAEA has found Iran in violation of nuclear obligations and issued a stern warning to Tehran in September. Thursday's vote would be the next step. Iran insists its nuclear program is intended only to produce electricity. The United States and some allies say Iran is hiding ambitions to build a nuclear bomb, but the Security Council members have been divided about how strong a line to take. Iran broke UN seals at a uranium enrichment plant Tuesday, January 10 and said it would resume nuclear fuel research after a two−year freeze. Tehran said the research would involve what it called limited uranium enrichment, but the action raised fears Tehran was using its pursuit of atomic power as a front for a nuclear weapons program.
Source: http://www.canada.com/topics/news/world/story.html?id=0ef0da 93−ca74−4315−82a7−0dcc0f964047&k=13210

6. *January 30, Mail & Guardian (Africa)* — **Theft of solar panels highlights infrastructure vulnerability.** A 2005 study indicated that up to 15 percent of solar panels installed in Senegal had been stolen. The study was released during a workshop held last month in the capital, Dakar, to discuss improving national and sub−regional strategies to fight solar−panel theft. Solar−panel theft has also affected the National Telecommunications Company and other government−run operations. During the past three years, more than 200 of the cells that make up solar panels installed have been stolen. According to the 2005 study, panels are sometimes stolen and sold by the engineers and technicians who installed them. In another instance, a Mauritanian national stole panels in Senegal for resale in his own country. Solar−panel thieves have targeted maternity hospitals, places of worship and schools in several villages across the interior of the country. While the 12 cells that make up a solar panel cost about $500 each, thieves sell them for about $200 in Senegal, or in neighboring countries. Oumar Top, secretary general in the agriculture and hydraulics ministry, has proposed that anti−theft devices for solar panels be used more widely −− particularly screw−in devices.
Source: http://www.mg.co.za/articlePage.aspx?articleid=262742&area=/ insight/insight__africa/

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *January 31, Associated Press* — **Six injured in North Carolina chemical plant explosion; residents urged to remain indoors.** An explosion at a chemical plant in Morganton, NC, left six people injured Tuesday, January 31, and nearby residents were urged to stay indoors until

officials determined the type of chemicals involved in the blast. At least two of the injured were taken to a hospital after the explosion at the Synthron Inc. plant shortly after 11:30 a.m. EST, officials said. Authorities called residents near the plant to tell them to close their windows and turn off their ventilation and heating systems while hazardous materials crews figure out what chemicals were possibly in the air, said Lisa Propst, a communications manager for Burke County emergency services. Officials don't know what caused the explosion, Propst said. Synthron is a subsidiary of Paris−based Protex International, a company that manufactures specialty chemicals in the United States, Europe, Asia and North Africa. Morganton is about 70 miles northwest of Charlotte, NC.
Source: http://wireservice.wired.com/wired/story.asp?section=Breakin g&storyId=1152329

8. *January 30, North County Times (CA)* — **Acid spill closes ramp on California interstate.** Spilled acid used to clean pools forced a half−hour shutdown Monday evening, January 30, of a southbound Interstate−5 ramp in Oceanside, CA, authorities said. Fire officials said a half−gallon of muriatic acid hit the pavement at the top of the ramp to Oceanside Boulevard just after 7 p.m. PST. "It was creating a cloud, so we diluted it with water and it went away," said fire Battalion Chief Bob Cotton.
Source: http://www.nctimes.com/articles/2006/01/31/news/coastal/1300 6213038.txt

[Return to top]

Defense Industrial Base Sector

9. *January 31, International Herald Tribune* — **With increased Chinese defense spending, rival nations ponder timetable for aircraft carrier acquisition.** As China builds a military to match its growing economic power, its neighbors and potential rivals including the U.S. have puzzled over a key question: When will the Chinese Navy launch an aircraft carrier? For decades, senior Chinese military and political officials have argued that for the country to become a great power, the People's Liberation Army Navy needs to add these potent warships to its fleet. However, the major obstacle to this ambition is that aircraft carriers are very expensive. And, aircraft carriers do not operate alone. They need a fleet of warships, submarines and supply vessels along with advanced electronic surveillance for support and protection. For these reasons, most experts assumed a Chinese carrier was decades away. But after double−digit increases in defense spending over much of the past 15 years, evidence is now emerging that China has a more ambitious timetable. Most naval experts agree that China will almost certainly build or buy aircraft carriers eventually. What is clear is that China has already invested decades of effort in its bid to gain the technology and skills needed to build and operate these warships.
Source: http://www.iht.com/articles/2006/01/30/business/carrier.php

10. *January 30, Reuters* — **Explosion at Florida defense contractor plant releases krypton gas.** An explosion on Monday, January 30, at a Jacksonville, FL, defense contractor plant that makes ignition systems for aircraft engines exposed at least 100 people to krypton gas and sent 12 to hospital for treatment, a fire department official said. The Unison Industries plant, a unit of General Electric, was quickly evacuated, Jacksonville fire−rescue spokesperson Bennie Seth said. Seventy−three people were found to be exposed to levels of radiation high enough that they had to be decontaminated, Seth said. Several hours after the explosion, gas levels in the

plant were found to be very low, she said. Unison employs about 500 people in the Jacksonville area but no more than 111 were located in the plant where Monday's incident occurred at about 10:45 a.m. EST, Milligan said. Seth said investigators had not yet found the cause of the blast. Krypton gas is colorless and nontoxic. It can be made artificially radioactive for use in manufacturing. The krypton at the plant was used for making medical supplies, according to Seth.
Additional information was found at:
http://www.guardian.co.uk/uslatest/story/0,,−5582712,00.html
Source: http://today.reuters.com/News/newsArticle.aspx?type=domesticNews&storyID=2006−01−30T195743Z_01_N30305137_RTRUKOC_0_US−EXPLOSION−GE.xml

[Return to top]

Banking and Finance Sector

11. *January 30, Internetnews.com* — **ID theft and Internet fraud declining?** Incidents of fraud from Internet−based means may well be on the decline. According to a report released Tuesday, January 31, by Javelin Strategy and Research, in cases where the source of the identity theft was known, only nine percent were reported to have come from hacking, viruses, and phishing. In contrast, a lost or stolen wallet or credit/debit card was the cause of 30 percent of the incidents. Also, fraudulent activity is mostly (over 70 percent) conducted offline via phone or mail. Average losses results from Internet−related identity theft fraud have ballooned over the last year to $6,432, up from $2,897. In the same period losses from ID theft taken from the garbage or mail have declined by 14 percent. Phishing was reported to have the highest average length of misuse at 173 days. Rubina Johannes of Javelin Strategy & Research said, "With the appropriate security and consumer education, phishing on existing accounts can be minimized...However, to stop phishing on new accounts is more difficult." Johannes added that, "Scammers are becoming more and more savvy in garnering seemingly innocuous pieces of personal information, which can then be used to open new, fraudulent accounts in the victims' names."
Source: http://www.internetnews.com/xSP/article.php/3581601

12. *January 30, Physorg.com* — **Second−hand computers pose identity theft threat.** A new identity theft study conducted by University of Leicester criminologist Professor Martin Gill found that second−hand computers −− which account for one in 12 computers in use worldwide −− can be a potential treasure trove of personal information −− putting users at risk of fraud and identity theft. The researchers purchased six used computers and conducted a forensic data analysis on each. Half of the computers had in fact not been securely wiped. In one case there had been no attempt to wipe the contents whatsoever. Gill said, "The fact that we found so much personal information through a focused study indicates that the potential for fraud and identity theft from the second hand PC market is huge...Simply re−formatting a hard drive is not enough to make data irretrievable. Anyone disposing of a personal computer must ensure that all data is securely wiped using specialist software to wipe over every sector of the hard drive." Among the data retrieved included: bank account details; correspondence with a bank noting change of e−mail address; sensitive information, including a spreadsheet which contained details of creditors, payroll, and the names and addresses of past and present business

customers.
Source: http://www.physorg.com/news10369.html

13. *January 30, Daily Gamecock (SC)* — **Officials warn of possible ATM scam.** The Crime Prevention Office of The University of South Carolina (USC) is warning students about an ATM scam that could come to the university. According to Cpl. Kenneth Adams, the scam involves the criminal slipping a small piece of plastic into the ATM that prevents the card from being expelled from the machine. The criminal then waits for someone to use the ATM. Once they lose their card in the machine, the crook approaches them and suggests that he knows how to get the card back. The criminal instructs the ATM patron to enter their PIN number while the criminal holds down both the "cancel" and "enter" keys. The criminal continues doing this until the victim's PIN number is memorized. After the victim becomes frustrated and leaves, the criminal pretends to do the same. But once the victim is out of sight the crook returns to the machine and removes the piece of plastic and the victim's ATM card along with it. Adams said USC received the scam alert through a network of shared information with other universities.
Source: http://www.dailygamecock.com/media/paper247/news/2006/01/30/News/Officials.Warn.Of.Possible.Atm.Scam−1520064.shtml?norewrite&sourcedomain=www.dailygamecock.com

[Return to top]

Transportation and Border Security Sector

14. *January 31, Seattle Post−Intelligencer (WA)* — **Airline rules spark safety concerns.** A federal rule permitting passengers to carry some previously banned items into aircraft cabins has touched off concerns about public safety. The Association of Flight Attendants held news conferences nationwide Monday, January 30, to draw attention to the Transportation Security Administration's (TSA) December 22 decision that allows people to carry on scissors with blades less than four inches and some tools, such as screwdrivers, wrenches or pliers, up to seven inches long. After the September 11, 2001, terrorist attacks, those items were banned from aircraft seating areas. TSA officials lifted that restriction primarily after determining that more federal attention was needed to detect someone trying to place explosives in airplanes.
Source: http://seattlepi.nwsource.com/business/257608_flightattendan ts31.html

15. *January 31, New York Times* — **A test at 25 stations: subway riding without the swiping.** On Monday, January 30, the Metropolitan Transportation Authority announced what could be a step in that direction: an experiment letting riders enter the subway by tapping or waving a credit card or payment tag. The six−month trial, scheduled to start this spring, could lend momentum to efforts toward a "smart card" valid on subways, buses and commuter trains throughout the region. The Port Authority of New York and New Jersey has championed that concept, but the transportation authority has been reluctant to embrace it. The experiment will involve a commercially available technology, the MasterCard PayPass, which can already be used at parking lots, fast−food restaurants, drug stores, gas stations and movie theaters. The PayPass comes in two forms ˜ a standard−size card or a tag that can be hung on a keychain ˜ and has an embedded microchip and radio antenna. The Citibank MasterCard PayPass will be accepted at 25 stations where turnstiles will have specially equipped readers. The PayPass functions like a normal credit or debit card, and the turnstile will be activated instantly, as with

a MetroCard.
Source: http://www.nytimes.com/2006/01/31/nyregion/31fare.html

16. *January 31, Agence France−Presse* — **Saboteurs caused Pakistani train crash: experts.** Pakistani investigators believe saboteurs tampered with a section of railway track, causing a train to plunge into a ravine and killing at least four people on Sunday, January 29, a minister said Monday, January 30. Experts found that nuts on the track had been unscrewed when they examined the site of Sunday's crash near the city of Jhelum in the eastern province of Punjab, Railways Minister Ishaq Khakwani said. Six cars of the express jumped the rails and three fell into the 50−foot gully around two hours after the Lahore−bound train left Rawalpindi, a city adjoining Islamabad. "It is almost confirmed now that it is an act of sabotage. The evidence says it is sabotage," Khakwani said. "We have seen spanners, the nuts of the fish plates were open," he added, referring to a key track part used to join different rail sections. The minister would not speak in detail about who might have sabotaged the track but said "several elements" could have been involved, adding: "It could be internal, it could be external." The death toll rose on Monday to four, while 94 people were injured, 10 of them seriously, railway police chief Zaheer Ahmed said.
Source: http://www.gulf−times.com/site/topics/article.asp?cu_no=2&item_no=70818&version=1&template_id=41&parent_id=23

17. *January 30, Associated Press* — **South Shore line to test wireless service.** Commuters on Chicago's South Shore rail system may soon be able to use their laptop computers and cell phones while riding the line between South Bend and Chicago. Officials at the Northern Indiana Commuter Transportation District say they're working on a deal to bring wireless service to commuters through the same technology used for communication in NASCAR racing. The service will be tested for 60 days, from April through June, on a seven−mile stretch from Dune Park to Ogden Dunes. The South Shore line would be the first commuter rail line in the nation to offer the service if the test is successful, railroad spokesperson Boris Matakovic said.
Source: http://www.chicagotribune.com/news/local/chi−060130southshore,1,7664366.story?coll=chi−news−hed

[Return to top]

Postal and Shipping Sector

18. *January 31, New York Times* — **Seven dead in California post office shooting.** A female ex−postal worker opened fire at a U.S. Postal Service mail processing plant in Goleta, CA, killing six people before committing suicide, authorities said early Tuesday, January 31. Deputies responding to a call of shots fired late Monday, January 30, initially found two people dead outside the plant. Two wounded women were located inside and were taken to a hospital. One died and the other was listed in critical condition early Tuesday with a gunshot wound to the head. During a search of the massive mail complex, deputies found four additional bodies, including one believed to be the female shooter, Santa Barbara County Sheriff Jim Anderson said. The shooter died of an apparent self−inflicted gunshot wound, he said. The postal station is located just a few blocks from the University of California, Santa Barbara, about 100 miles northwest of Los Angeles.

Source: http://www.nytimes.com/aponline/national/AP−Post−Office−Shooting.html?hp&ex=1138770000&en=bcd2df50eb399395&ei=5094&partn er=homepage

[Return to top]

Agriculture Sector

19. *January 31, Animal and Plant Health Inspection Service* — **License issued for plant−cell produced Newcastle disease vaccine.** The U.S. Department of Agriculture (USDA) Tuesday, January 31, announced that it has issued a license to Dow AgroSciences LLC for a vaccine to protect chickens from illness caused by the Newcastle disease virus (NDV). The chicken vaccine is the first fully licensed plant−cell produced vaccine for animals in the U.S. and the first plant−made product to be licensed by USDA's Animal and Plant Health Inspection Service (APHIS). The vaccine contains the major immunogenic protein of the NDV and does not contain any whole NDV, live or killed. Once the chicken's cells take up the protein in the vaccine, they trigger a protective immune response. In granting full licensure, APHIS' Center for Veterinary Biologics determined that the vaccine's safety and efficacy have been satisfactorily demonstrated. NDV occurs in many species of birds, is transmitted by inhalation and ingestion and displays wide variation in pathogenicity among strains. NDV can be either neurotropic or viscerotropic. The neurotropic viruses cause respiratory and nervous signs. The viscerotropic viruses, which are more common, result in respiratory signs, diarrhea and swelling of the head and neck.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/ndvaccine .shtml

20. *January 31, Stop Soybean Rust News* — **Soybean rust found in kudzu patch in Georgia.** Soybean rust was found Monday, January 30, on old kudzu leaves that appear to have survived cold temperatures in southern Georgia. Grady County becomes the first county in Georgia to have rust in 2006 and brings the U.S. total to a dozen counties in three states this year. Layla Sconyers, with the department of plant pathology of the University of Georgia, reported that the infected patch of kudzu was found behind a building in downtown Cairo, GA, near the Georgia/Florida border. The rust was found on what appeared to be older leaves that had survived the cold temperatures thanks to protection from the building. "Copius amounts of rust pustules and spores were observed later at a laboratory dissecting microscope at the University of Georgia Coastal Plain Experiment Station," Sconyers said.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=681

21. *January 30, Animal and Plant Health Inspection Service* — **Second phase of enforcement for wood packaging material import regulations.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) in cooperation with the U.S. Department of Homeland Security's Customs and Border Protection (CBP) will begin enforcing phase two of the new wood packaging material (WPM) regulation beginning February 1. During this phase, APHIS and CBP will require that all commodity imports entering or transiting the U.S. with WPM consisting of pallets and crates be either heat treated or fumigated with methyl bromide. The shipments must also be marked with an approved international logo, certifying that the WPM has been appropriately treated. WPM that does not meet these requirements will not be allowed to enter into the U.S. and will be re−exported. Shipments containing WPM that violate the rule may be allowed entry only if the CBP port director determines that it is possible to

separate the approved material from the noncompliant portion of the shipment. Arrangements to have the noncompliant WPM exported from the U.S. would be required before the approved cargo can be released to the consignee. All costs associated with this process are the responsibility of the importer.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/wpmsecpha se.shtml

22. *January 30, Animal and Plant Health Inspection Service* — **Regulations regarding Minnesota's bovine tuberculosis status amended.** The U. S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending the bovine tuberculosis (TB) regulations regarding state and zone classifications by removing Minnesota from the list of accredited−free states and adding it to the list of modified accredited advanced states. Prior to this interim rule, Minnesota was designated as accredited free. However, five TB−infected herds have recently been detected in Minnesota. Federal regulations require that if two or more cattle herds are detected in an accredited−free state or zone within a 48−month period, the state or zone will be removed from the list of accredited−free states or zones and will be reclassified as modified accredited advanced. As a result of Minnesota's reclassification as a modified accredited advanced state, the movement of cattle, bison and captive cervids moving from Minnesota will be restricted, according to federal regulations, in order to prevent the spread of TB, a contagious and infectious disease caused by Mycobacterium bovis. The disease affects cattle, bison, deer, elk, goats and other warm−blooded species, and can be fatal.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/mntbstate .shtml

[Return to top]

Food Sector

23. *January 31, Agence France−Presse* — **Majority of Japanese back U.S. beef ban.** An overwhelming majority of Japanese support the decision to ban U.S. beef imports for violating a food safety agreement and most want tighter restrictions if imports resume, a new poll revealed. Some 87 percent backed the new ban, which was imposed only a month after U.S. beef was allowed to return to the market, against eight percent who opposed it, said the Asahi Shimbun poll of 1,915 Japanese adults. However, people were sharply divided over the original decision to lift the embargo, with 48 percent believing it was too early against 45 percent who thought it was appropriate. Japan, formerly the top overseas market for U.S. beef, in December resumed imports, which were suspended in 2003 after a mad−cow case was discovered in a herd in Washington state. On January 20, however, Japan found that a U.S. shipment that arrived near Tokyo contained spinal columns, which are forbidden as a precaution against mad−cow disease, and imposed a new ban. Some 57 percent want the government to impose tougher conditions if resuming U.S. beef imports against 33 percent who are satisfied with the current rules, the poll said.
Source: http://news.yahoo.com/s/afp/20060131/hl_afp/japanpoliticsust radehealthmadcow_060131070753;_ylt=AittO4qhKW.p3R9Ssf4_5SKJO rgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

24. *January 30, WIS (SC)* — **Preliminary report suggests decayed gasoline as cause for milk contamination.** According to a preliminary report by the South Carolina Department of Health & Environmental Control (DHEC), the cause of the milk contamination in the Barnwell school

district was decayed gasoline. They believe the decayed gasoline was on the cartons, and that it was possible that it could have seeped into the milk through the cardboard carton. In early January, staff and students noticed a strange odor coming from the milk or carton. It was a strong odor, but not that of spoiled milk. They notified DHEC, which investigated and tested samples for contamination. DHEC also went to the Coburg milk plant, where they happened to still have some of the milk from the same lot. That milk did not have an odor and tested out fine. There were no reports of anyone becoming sick.
Source: http://www.wistv.com/Global/story.asp?S=4428915&nav=0RaP

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

25. *January 31, Associated Press* — **Tally of human bird flu cases rises to 160.** The World Health Organization (WHO) on Tuesday, January 31, raised to 160 its official tally of people worldwide who have been infected with the H5N1 strain of bird flu virus after laboratory tests in England confirmed that at least 12 people in Turkey have been infected with the disease. The death toll from the disease has risen to 85, including four in Turkey, the WHO said. Nine further samples, from individuals confirmed by Turkish health officials as H5N1 positive, are still being examined in England to verify that they carried the disease, said WHO spokesperson Iain Simpson. WHO does not officially update its tally of confirmed cases until the disease has been verified in a laboratory outside the country of the outbreak, meaning that WHO's figures often lag behind national counts.
Cumulative Number of Human Cases of Avian Influenza Reported to WHO:
http://www.who.int/csr/disease/avian_influenza/country/cases_table_2006_01_30/en/index.html
Source: http://www.nola.com/newsflash/international/index.ssf?/base/international-2/1138709970155480.xml&storylist=international

26. *January 31, Agence France-Presse* — **Iraqi Kurdistan faces acute shortage of bird flu drug.** Iraq's Kurdistan region, which has confirmed its first human death from bird flu, is facing an acute shortage of the vital drug to fight the disease, a medical official said. "We are suffering from a lack of medicine to combat the virus," Tahseen Nameq, head of a joint Kurdish committee set up to combat the spread of the disease, said on Tuesday, January 31. "We have received only 50 pills of Tamiflu," he said. A single course of medicine per patient consists of two pills a day for five days, giving the whole Kurdish region in northern Iraq enough medicine for five cases. Health Minister Abdel Mutalib Mohammed Ali said the government was mobilizing to contain the crisis. "We are going to meet all of Kurdistan's needs because we want to control the situation and we are convinced we can," he said at a press conference in Sulaimaniyah, adding that five mobile hospitals had been sent to the three Kurdish provinces. Kurdistan has quarantined 14 people suspected of suffering from bird flu, but officials say that

other than the fatality, only one other case is truly suspected to be the H5N1 strain. Source: http://news.yahoo.com/s/afp/20060131/wl_mideast_afp/healthfl uiraq_060131130846

27. *January 30, University of Texas Southwestern Medical Center* — **Human trial proves ricin vaccine safe.** Scientists have completed the first human clinical trial of a recombinant vaccine for the deadly toxin ricin −− a potential bioterror threat −− and the results indicate the vaccine is safe and effective in eliciting ricin−neutralizing antibodies, the University of Texas Southwestern Medical Center researchers report. The nearly year−long pilot study involved three groups of five volunteers each. Individuals in each group received a series of three injections of various doses of the vaccine, called RiVax, over the study period. As a recombinant vaccine, RiVax is a form of ricin that consists of a genetically modified subunit of the toxin, rather than an inactivated whole toxin. All five of the individuals in the group receiving the highest vaccine dose produced ricin−neutralizing antibodies in their blood, indicating their immune systems had responded. Four of five in the intermediate dose group produced antibodies, while one of five in the lowest dose group did so. The human−produced antibodies were then injected along with active ricin toxin into test mice, and the mice survived. Source: http://www8.utsouthwestern.edu/utsw/cda/dept37389/files/2711 61.html

28. *January 30, University of California, San Diego* — **Study finds anthrax toxins also harmful to fruit flies.** Deadly and damaging toxins that allow anthrax to cause disease and death in mammals have similar toxic effects in fruit flies, according to a study conducted by biologists at the University of California, San Diego. Their findings show that fruit flies can be used to study the link between the biochemical activities and physiological effects of anthrax toxins. Learning how these toxins attack developing and adult tissues is important because it can help scientists understand how they function at the molecular level and may lead to new therapeutic strategies for neutralizing their effects in humans. Researchers tracked the ways that two active anthrax toxins, known as lethal factor (LF) and edema factor (EF) cause cellular damage and death in the fruit fly Drosophila melanogaster. These toxins are required for the anthrax bacterium Bacillus anthracis to evade the host immune system and cause disease. Using a combination of biochemical, genetic and cell biological approaches, the biologists tested whether or not the anthrax toxins were active in living Drosophila and, if so, whether they acted in the same way as they do in humans. The biologists found that anthrax toxins do alter the same signaling pathways used for cell communication in fruit flies and humans. Source: http://ucsdnews.ucsd.edu/newsrel/science/mcanthrax.asp

29. *January 30, Associated Press* — **Connecticut program launched to store and share medical records electronically.** Within the next few years, Connecticut patients' medical records could be electronically accessible around the clock to doctors, hospitals, and other health care providers statewide. Governor M. Jodi Rell and U.S. Rep. Nancy Johnson on Monday, January 30, joined a coalition of health care professionals to announce the launch of eHealth Connecticut, an initiative to store and share medical records over an electronic network in place of today's paper−based methods. They say it could help reduce prescription errors, provide better information during emergencies and save money by alerting physicians to medical procedures that already have been conducted and do not need to be repeated. "It will let doctors and hospitals communicate more rapidly, more effectively, in real time," Rell said. "That's what we want, not two−day−old information or having to send somebody back for a different test −− real time, right now." For example, emergency room doctors could quickly check a patient's

medical history, prescriptions, potential allergies and other critical information even if the patient cannot talk and his or her doctor's office is closed for the night. Coalition officials said they expect the statewide electronic record−sharing system to start operating within the next two years if all remains on schedule.
Source: http://www.boston.com/news/local/connecticut/articles/2006/01/30/connecticut_program_launched_to_store_and_share_medical_records_electronically/

30. *January 30, Brownsville Herald (TX)* — **Drug−resistant tuberculosis worries officials.** In Mexico, anyone can pick up the antibiotic telithromycin or other potent antibacterial drugs such as rifampin to treat tuberculosis (TB). Easy dispensation of these drugs frustrates health officials, who say short−term and inconsistent medication use creates a drug−resistant variety of the life−threatening illness. The drug−resistant TB variation is costlier and takes longer to treat, hurting already strained federal and state budgets. And if resources are limited in treating normal TB cases, drug−resistant and the even more serious multi−drug resistant cases will only multiply. Drug resistance stemming from immigration from countries with lax TB treatment enforcement by the government and private physicians, and intravenous drug use and alcohol abuse in a transient population have contributed to making TB a potential health crisis. MDR−TB incidents still comprise a small portion of TB cases but increased diagnosis in Texas means more drug−resistant cases are inevitable. In 2004, the Hildago, TX, health department handled 101 new cases of TB, a 25 percent increase from 2004. It costs the state about $2,800 and takes six to nine months to treat a standard TB patient. An MDR−TB client, on the other hand, has treatment costs running about $250,000 for the two−year duration of the treatment.
Source: http://www.brownsvilleherald.com/ts_more.php?id=69075_0_10_0_M

[Return to top]

Government Sector

31. *January 31, Northeast Georgian (GA)* — **Courthouse metal detector to be put into use next week.** Following the Atlanta courthouse shootings in March 2005, security measures in many Georgia county, state, and federal buildings have been increased. Beginning February 6, everyone entering the Habersham County Courthouse in Clarkesville will be subject to search by Habersham County Sheriff's deputies if a new metal detector located at the front entrance to the courthouse on Highway 115 warns officials of possible weapons or other suspicious objects. “Everybody, even if you're an employee in the courthouse, is going through this,” Habersham County Sheriff DeRay Fincher says. “The minute you start exempting people you don't have a security system. That's the only way to have maximum security.” Signs already are posted on the courthouse doors alerting those entering to leave at−risk items in their vehicles. Besides firearms, the list also includes pocketknives and pepper spray. The state−of−the art detector alerts deputies on duty not only with sound when metal is detected, but also with red sensors along the edge of the machine. . Security cameras and monitors also are in place. Fincher points out his department worked with the county judges to implement a system and policy to best fit Habersham County.
Source: http://www.thenortheastgeorgian.com/articles/2006/01/31/news/top_stories/01topstory.txt

[Return to top]

Emergency Services Sector

32. *January 30, Federal Times* — **A lesson from Katrina: Learn text messaging.** If there's one simple goal federal managers ought to accomplish before a natural disaster, it's this: Learn to use text messaging. When cell phone service was disrupted by Hurricane Katrina, the low−bandwidth burps of short text messages were often the only way to communicate in the devastated areas of Louisiana, a panel of government and private−sector officials told an audience of chief information officers. John Lawson, the chief information officer of Tulane University in New Orleans, described two cell phones he used during Katrina: Each operates over a different service network, but in the storm's aftermath, neither could keep a signal long enough to make a voice call. "The entire 504 area code went down," Lawson said. "It was very difficult for me to get through to my directors. Text messaging works, and I encourage your execs to learn text messaging, because that was what worked." Capt. Joe Castillo of the Coast Guard's 8th District echoed the thought. "It was our younger folks who figured that out...It worked very well." In addition to text messages, the 8th District set up free e−mail accounts on the Web. "Coastguardplans@yahoo.com became the central planning place," said Castillo.
Source: http://federaltimes.com/index.php?S=1499933

33. *January 30, Washington Technology* — **Identity management within interoperable networks may hamper first responders' efforts.** First responders soon may need more than a radio or a password to access interoperable networks under development: They will need to verify their identities. The federal smart−card regulations anticipated under Homeland Security Presidential Directive−12 (HSPD−12) are adding layers of complexity to the already difficult goal of strengthening public safety communications by making radios and networks more interoperable with each other. As public safety networks become more sophisticated and gain access to more databases and networks, there's now a need to integrate and simplify identity management, so that first responders aren't slowed in doing their jobs by a need to remember and enter excessive personal identification numbers and passwords. The smart−card solutions envisioned under HSPD−12 typically include a plastic card with a radio frequency identification chip or magnetic tape containing biometric information that must be swiped or read by a reader. These methods do not "always work in a rapid, highly mobile responder environment," according to Bill Wagner, director of interoperability and information sharing for AT&T Corp.'s government solutions unit. An alternative that AT&T is examining is voice recognition, which is easier and quicker to use than a smart card, he said.
Source: http://www.washingtontechnology.com/news/21_02/federal/27847−1.html

34. *January 30, WLS−TV/DT Chicago* — **New emergency management center unveiled in Chicago.** Monday morning, January 30, Chicago officials unveiled a new $4 million high−tech emergency management center. It will streamline the city's response to everything from snowstorms to possible terrorist attacks. Twenty−four high−tech workstations coordinate the city departments that handle emergencies and disasters. Twelve big−screen TV's hang down from the ceiling to display images from weather and news sources, and hundreds of surveillance cameras around the city. In addition, the center has a high−resolution digital video capable of displaying images from multiple sources, and one wall has a movable track that shuttles TV monitors to work stations around the room. "This is a logical next step in our effort to effectively respond to emergencies on a city−wide basis," said Andrew Velasquez,

emergency center director. City officials claim Chicago has the most sophisticated high−tech emergency communication system in the country, along with enough trained personnel to operate it well with no additional cost to the taxpayers.
Source: http://abclocal.go.com/wls/story?section=local&id=3860201

35. *January 30, National Journal* — **FCC panel convenes Katrina communications probe.** The Federal Communications Commission (FCC) on Monday, January 30, opened an independent panel investigation into the effect of Hurricane Katrina on the nation's communications systems. The panel, which includes members from private and public organizations, has been charged with providing the agency with a list of recommendations by June 15 on how to improve the nation's emergency response and communications systems. Panel Chairwoman Nancy Victory said the investigation would be split into three working groups focusing on infrastructure resiliency, recovery coordination and procedures and emergency communications. The working groups will conduct their own research and collect testimony in between the full panel's meetings before the final report's June deadline. Democratic Commissioner Michael Copps stressed the importance of allowing a broad range of voices to be heard during the investigation. He specifically asked panelists to pay attention to the needs of the disabled, who have no direct representation on the panel. FCC Chairman Kevin J. Martin said there would be opportunities for groups not included on the panel to provide testimony to the working groups, and that the commission would keep the process as open as possible.
Source: http://www.govexec.com/dailyfed/0106/013006tdpm1.htm

[Return to top]

Information Technology and Telecommunications Sector

36. *January 31, Secunia* — **Winamp computer name handling buffer overflow vulnerability.** ATmaCA has discovered a vulnerability in Winamp, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error during the handling of filenames including a computer name. This can be exploited to cause a buffer overflow via a specially crafted playlist containing a filename starting with an overly long computer name (about 1040 bytes). Solution: Update to version 5.13.
Source: http://secunia.com/advisories/18649/

37. *January 30, Security Focus* — **Mozilla Firefox XBL −MOZ−BINDING property cross domain scripting vulnerability.** The Mozilla and Mozilla Firefox browsers are vulnerable to a cross domain scripting attack by which a malicious Webpage could access trusted sites' properties and execute arbitrary script code in the context of an arbitrary domain. The issue affects the "−moz−binding" property supported by the Mozilla Extensible Binding Language. XBL is a markup language for describing bindings that can be attached to elements in other documents. Bindings can be attached to elements using either cascading stylesheets [CSS] or the document object model [DOM]. A malicious site could access the properties of a trusted site and facilitate various attacks including disclosure of sensitive information.
Source: http://www.securityfocus.com/bid/16427/references

38. *January 30, IDG News Service* — **Hackers lurk in AMD Website.** Advanced Micro Devices

(AMD) Inc.'s customer support discussion forums on the forums.amd.com site have been compromised and are being used in an attempt to infect visitors with malicious software, an AMD spokesperson confirmed Monday, January 30. The problem was first reported Monday in a blog posting by Mikko Hypponen, manager of antivirus research at F−Secure Corp. in Helsinki. According to F−Secure's Hypponen, attackers are exploiting a widely reported flaw in the way the Windows operating system renders images that use the WMF (Windows Metafile) graphics format. This flaw was patched on January 5, so users who are running versions of Windows that have the latest patches installed are not at risk, he said. Attackers have figured out a way to use AMD's forums to deliver maliciously encoded WMF images to visitors, which are then used to install unauthorized software on the unpatched systems, he said. "Most of the tool bars show pop−ups, follow your search and other keyword activity, and use that to target ads to you," Hypponen said. "It's for−profit hacking. Somebody is making money from each machine that is hit by these tool bars."
Source: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,108195,00.html

39. *January 30, Tech Web* — **Kama Sutra worm hits India, Peru hardest.** The worm set to overwrite important Microsoft and Adobe documents Friday, February 3, has struck India five times harder than the U.S., and Peru three times harder, a security company claimed. According to Chicago−based LURHQ, the worm −− dubbed Kama Sutra, Blackworm, Blackmal, MyWife, Nyxem, and nearly two−dozen other names −− has infected nearly 80,000 PCs in India. Peru sports almost 55,000 compromised computers. In comparison, the U.S. has about 15,000 machines contaminated with the worm. "Viruses don't always spread uniformly," LURHQ said in its report. "There are many factors at play which are hard to quantitize, such as the initial seeding, social engineering, AV deployment, and random chance. And, as with all statistics, take [these] with a grain of salt." LURHQ tagged the total number of Blackworm−infected computers at around 300,000, even though a Web−based infection counter claims a number in the millions. LURHQ, however, was able to strip out bogus "clicks" on that counter to arrive at is estimate. "An attempt was made by an unknown party to artificially inflate the counter using a set of 279 distributed (presumably compromised) computers," said LURHQ.
LURHQ's report: http://www.lurhq.com/blackworm−stats.html
Source: http://www.techweb.com/wire/security/177105325;jsessionid=FICPCUF4MHL4YQSNDBOCKHSCJUMEKJVN

40. *January 30, Register (United Kingdom)* — **Security vendors open another front against spyware.** The three biggest anti−virus vendors have teamed up with testing labs to develop standards for spyware detection. Trend Micro, Symantec and McAfee are joining forces with ICSA Labs and Thompson Cyber Security Labs in a bid to standardize methods for sharing spyware samples and testing anti−spyware products and services. The effort is aimed at curtailing a possible source of user confusion before it becomes a problem, as well as driving up standards for detection across the anti−spyware industry. Spyware testing, modeled on schemes the anti−virus industry has been running for years, will also make it easier to compare the efficacy of various anti−spyware products, at least in theory. The group’s anti−spyware testing methodology and best practices can be viewed at Spywaretesting.org. The initiative is one of a number of cross industry efforts aimed at coordinating the fight against spyware −− the invasive programs that track user's surfing habits or, in the worst cases, steal their personal information, such as credit card or Social Security numbers.

Spywaretesting Website: http://www.spywaretesting.org/metadot/index.pl
Source: http://www.theregister.co.uk/2006/01/30/spyware_testing/

41. *January 30, ZDNet News* — **Microsoft patent spat forces businesses to upgrade Office.** Microsoft has begun e−mailing its corporate customers worldwide, letting them know that they may need to start using a different version of Office as a result of a recent legal setback. The software maker said Monday, January 30, that it has been forced to issue new versions of Office 2003 and Office XP, which change the way Microsoft's Access database interacts with its Excel spreadsheet. The move follows a verdict last year by a jury in Orange County, CA, which found in favor of a patent claim by Guatemalan inventor Carlos Armando Amado. Microsoft was ordered to pay $8.9 million in damages for infringing Amado's 1994 patent. That award covered sales of Office between March 1997 and July 2003. Although existing customers can keep using older versions on current machines, any new installations of Office 2003 will require Service Pack 2, released by Microsoft in September. Office XP will need to be put into use with a special patch applied. The software maker started notifying customers this month, in an e−mail sent via its sales channel. All those affected will have been informed by next month, Microsoft said. The company said the necessary downloads are available from its Website.
Source: http://news.zdnet.com/2100−3513_22−6032870.html

42. *January 30, Washington Technology* — **DHS, agencies plan joint Cyber Storm exercise.** The Department of Homeland Security (DHS) will test how well it works with other federal agencies and private IT companies to protect cybersecurity in a national exercise from February 6−10. The Information Technology Information−Sharing and Analysis Center will take part in the exercise, known as “Cyber Storm,” with DHS to test its draft concept of operations for responding to cybersecurity incidents. Participating in Cyber Storm are Cisco Systems Inc., Citadel Security Software Inc., Computer Associates International Inc., Computer Sciences Corp., Intel Corp., Microsoft Corp., Symantec Corp., and VeriSign Inc., the center announced on its Website. Cyber Storm also will involve government agencies. According to Donald Purdy, acting director of DHS’ National Cyber Security Division, the division established the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation for readiness and response. The teams, comprising government computer experts, are responsible for IT security at government agencies. In addition to the GFIRST teams, the agency has worked with the Defense and Justice departments to form the National Cyber Response Coordination Group to provide an organized federal response to cybersecurity breaches.
Source: http://www.washingtontechnology.com/news/1_1/daily_news/27877−1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is receiving reports of a new destructive email worm known as CME 24, which will actively disable anti−virus software on a host system and will also overwrite users' data files on the third of every month. This worm affects all recent versions of Microsoft Windows. CME 24 is also known as Nyxem.E, Blackmal.E, MyWife.d, BlackWorm, Tearec.A, Grew.a, and Kama Sutra.

This malcode spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp.

Agencies that observe communication from internal machines to the 207.172.16.155 address should investigate further to determine if these machines are infected. Several agencies have reported that the systems that were impacted had anti−virus but were not running the latest signatures.

US−CERT recommends the following course of action:

Ensure that the latest anti−virus definitions are loaded on servers and workstations.

Leverage Internet Content Filtering Solutions to block executable and unknown file types at the email gateway

Setting up an access control list to detect users from browsing to the aforementioned websites/IP addresses. LURHQ provides snort signatures related to the CME−24 worm on their Website.

Monitoring of outbound traffic to identify potential malicious traffic or information leaks.

The infected host will also access a website with a web counter. This web counter shows how many machines have been infected, although it is expected that an infected machine may access the website on multiple occasions, thus inflating the number. The original web counter showed consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. However, recent web log postings suggest that the number is much closer to 300,000 unique addresses. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

Please report any validated agency connection to the 207.172.16.155 website during the last 30 days to the US−CERT for further correlation and analysis.

Nyxem Mass−mailing Worm US−CERT is aware of a new mass mailing worm known as Nyxem (CME−24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.The Nyxem worm targets Windows systems that hide file extensions for known file types (this is the default setting for Windows XP and possibly other versions). The worm's icon makes it appear to be a WinZip file. As a result, the user may unknowingly execute the worm. For more information please review: http://cme.mitre.org/data/list.html#24

US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. Users may also wish to visit the US−CERT Computer Virus Resources for general virus protection information at URL: http://www.us−cert.gov/other_sources/viruses.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 27015 (halflife), 445 (microsoft−ds), 32768 (HackersParadise), 139 (netbios−ssn), 135 (epmap), 80 (www), 26638 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

43. *January 31, Sacbee (CA)* — **Chemical fog forces evacuation at mosque in California.** Police and fire officials investigated a suspicious plume of fog in Sacramento, CA, Monday afternoon, January 30, in the Downtown Masjid at Fourth and V streets, and evacuated surrounding residences, officials said. Police spokesperson Sgt. Terrell Marshall said no injuries were reported as a result of the detonation at the Muslim mosque, but 20 to 30 residents had to be evacuated from the area until the nature of the substance was determined. Fire Capt. Niko King said firefighters with training in hazardous materials determined that the chemical came from a portable fire extinguisher. Marshall said a woman entered the mosque about 3 p.m. PST and detonated a device that released fog. He said one man, who was praying in the mosque, witnessed the event and promptly left the building. The woman was described as about five feet tall, 30 to 50 years old, with slender build with reddish hair, and wearing a black coat, black tights, and a green scarf, he said.
Source: http://www.sacbee.com/content/news/religion/story/14135912p− 14964735c.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer